Method and device for verifying IC cards

Patent number:	EP0203543
Publication date:	1986-12-03
Inventor:	KRIVACHY THOMAS DR-PHIL
Applicant:	SIEMENS AG (DE)
Classification:	
- international:	G07F7/10
- european:	G07F7/08E; G07F7/10D4
Application number:	EP19860106997 19860523
Priority number(s):	DE19853519554 19850531

Also published as:

EP0203543 (A3)
EP0203543 (B2)
EP0203543 (B1)

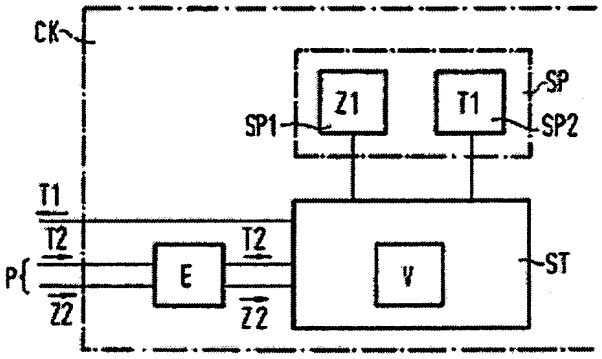
Cited documents:

EP0138386
US4105156

Report a data error here

Abstract of **EP0203543**

The verification of IC cards (CK) for authority to have access to an IC card system is carried out by allocating to a subscriber not only a fixed subscriber number (T1) or account number, but also a state number (Z1) unknown to him. The state number (Z1) is stored on the IC card in such a way that it cannot be read off from outside. To verify authorisation, the state number (Z2) is fed to the IC card from the central station or a terminal and is compared on the IC card with the state number (Z1) stored there. In addition to the state number (Z1), the subscriber number (T1) can also be compared. The state number (Z2) and, if appropriate, the subscriber number (T2) can be transmitted in coded form to the IC card.



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 203 543**
A2

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **86106997.9**

(51) Int. Cl.⁴: **G07F 7/10**

(22) Anmeldetag: **23.05.86**

(30) Priorität: **31.05.85 DE 3519554**

(43) Veröffentlichungstag der Anmeldung:
03.12.86 Patentblatt 86/49

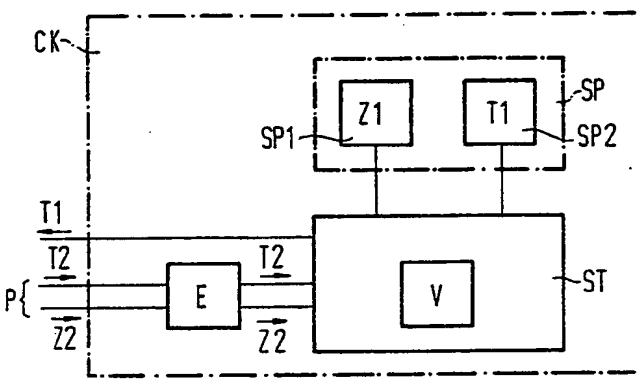
(84) Benannte Vertragsstaaten:
DE FR GB IT SE

(71) Anmelder: **Siemens Aktiengesellschaft Berlin und München**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Krivachy, Thomas, Dr.-Phil.**
Buchauerstrasse 39
D-8000 München 71(DE)

(54) Verfahren und Anordnung zum Überprüfen von Chipkarten.

(57) Die Überprüfung von Chipkarten (CK) hinsichtlich der Berechtigung des Zugangs zu einem Chipkartensystem erfolgt dadurch, daß einem Teilnehmer neben einer festen Teilnehmernummer (T1) oder Kontonummer eine ihm unbekannte Zustandsnummer - (Z1) zugeteilt wird. Die Zustandsnummer (Z1) ist auf der Chipkarte (CK) derart gespeichert, daß sie nicht von außen ausgelesen werden kann. Zur Überprüfung der Berechtigung wird der Chipkarte - (CK) von der Zentralstelle oder einem Endgerät die Zustandsnummer (Z2) zugeführtund auf der Chipkarte (CK) mit der dort gespeicherten Zustandsnummer (Z1) verglichen. Zusätzlich zu der Zustandsnummer (Z1) kann auch die Teilnehmernummer - (T1) verglichen werden. Die Zustandsnummer (Z2) und gegebenenfalls die Teilnehmernummer (T2) können verschlüsuselt zur Chipkarte (CK) übertragen werden.



EP 0 203 543 A2

Verfahren und Anordnung zum Überprüfen von Chipkarten

Die Erfindung bezieht sich auf ein Verfahren zum Überprüfen von Chipkarten entsprechend dem Oberbegriff des Patentanspruches 1. Weiterhin bezieht sich die Erfindung auf eine Anordnung zur Durchführung des Verfahrens.

Es ist bereits allgemein bekannt, Chipkarten als elektronisches Zahlungsmittel zu verwenden. Die Chipkarten werden beispielsweise an sogenannten POS (Point of Sales)-Endgeräten oder an öffentlichen Kartentelefonen benutzt. Die Chipkarten enthalten mindestens einen integrierten Schaltkreis, der als Speicherschaltkreis und/oder als Schaltkreis mit zusätzlichen Logikfunktionen, beispielsweise als Mikrorechner ausgebildet sein kann.

Wenn Chipkarten als elektronisches Zahlungsmittel oder auch als Berechtigungskarten für den Zugriff zu bestimmten Daten verwendet werden, werden aus Sicherheitsgründen die Chipkarten in Sperrdateien auf ihre Echtheit und Gültigkeit überprüft. Bei Verlust der Chipkarte meldet der Kunde seine Konto-oder Teilnehmernummer an den Systembetreiber, der diese Nummer dann sperrt und dem Kunden eine neue Nummer zuteilt. Bei bestimmten Nummern, z.B. der Fernmeldekontonummer, Personalnummer einer Firma oder Versicherungsnummer ist eine Änderung der Nummer oft mit erheblichem Aufwand verbunden oder unmöglich.

Chipkarten mit einer festen von einer Bank vorgegebenen persönlichen Identifikationsnummer (PIN) und einer vom Kunden individuell wählbaren Nummer sind üblich. Die vom Kunden individuell wählbare Nummer kann dabei mehrmals geändert werden, ohne daß die Teilnehmernummer geändert werden muß. Die persönliche Nummer ist jedoch nicht auf der Chipkarte gespeichert, sondern sie muß von dem Benutzer an dem Endgerät eingegeben werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Überprüfen der Gültigkeit von Chipkarten anzugeben, bei dem die Sicherheit weiter erhöht wird, ohne daß bei dem Verlust einer Chipkarte die Teilnehmernummer geändert werden muß.

Erfindungsgemäß wird die Aufgabe bei dem Verfahren der eingangs genannten Art durch die im kennzeichnenden Teil des Patentanspruchs 1 angegebenen Merkmale gelöst.

Sowohl dem Chipkartensystem als auch der Chipkarte sind sowohl die Teilnehmernummer als auch die Zustandsnummer bekannt, wogegen der Kunde nur die Teilnehmernummer kennt. Die heutige Technologie ermöglicht es, auf den Chipkarten Speicherbereiche festzulegen, deren Daten niemals gelöscht, geändert oder ausgelesen werden können, die aber auf der Chipkarte einen Vergleich zwischen einer eingegebenen und der abgespeicherten Nummer durchführen. Im Sinne der Erfindung bedeutet das, daß die Zustandsnummer von niemandem ausgelesen und damit kein Mißbrauch betrieben werden kann. Falls der Kunde veranlaßt, daß die ihm ausgegebene Chipkarte gesperrt werden soll, weil er sie verloren hat oder weil der Verdacht auf Vorhandensein einer weiteren, aber gefälschten Karte besteht, dann kann er gemäß der Erfindung eine neue Chipkarte mit der ursprünglichen Teilnehmernummer aber mit einer anderen Zustandsnummer erhalten.

Bei einer bevorzugten Ausführungsform der Erfindung wird auf der Chipkarte nicht nur die Zustandsnummer, sondern auch die Teilnehmernummer mit einer zur Chipkarte übertragenen Prüfnummer verglichen.

Die Zustandsnummer enthält mindestens ein Bit. Aus Sicherheitsgründen ist es jedoch empfehlenswert, daß die Zustandsnummer mindestens zwei Binärzeichen umfaßt. Aus Sicherheitsgründen können die Zustandsnummern statistisch vergeben werden, d. h. bei Verlust einer Chipkarte wird bei der neuen Chipkarte die Zustandsnummer nicht um 1 erhöht oder erniedrigt, sondern statistisch ausgewählt.

Zur Erhöhung der Sicherheit wird in einer weiteren Variante der Erfindung die zur Chipkarte übertragene Prüfnummer, bestehend aus der Teilnehmernummer und der variablen Zustandsnummer oder nur die Zustandsnummer nicht im Klartext, sondern verschlüsselt übertragen. Auf der Chipkarte wird die Prüfnummer dann entschlüsselt und die Zustandsnummer und gegebenenfalls auch die Teilnehmernummer wird mit der dort gespeicherten Zustandsnummer bzw. Teilnehmernummer verglichen. In der Sperrdatei ist der Schlüssel für jeden Teilnehmer bekannt und der verschlüsselte Text kann in Klartext umgewandelt werden.

Eine bevorzugte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß auf der Chipkarte ein Speicher mit einem von außen unzugänglichen ersten Speicherbereich für die Zustandsnummer und einem zweiten Speicherbereich für die Teilnehmernummer und eine Steuereinheit vorgesehen sind, die eine eingegebene Prüfnummer mit der Zustandsnummer vergleicht und ein Vergleichssignal abgibt.

Zur Entschlüsselung der zur Chipkarte übertragenen Prüfnummer, zumindest der Zustandsnummer ist bei einer weiteren bevorzugten Ausführungsform eine Entschlüsselungseinrichtung auf der Chipkarte vorgesehen.

Eine Durchführung des Verfahrens gemäß der Erfindung wird im folgenden anhand einer Anordnung näher beschrieben.

Die Figur zeigt ein Blockschaltbild einer Chipkarte.

Die Chipkarte CK ist in bekannter Weise mit einem elektronischen Schaltkreis versehen, der als Speicherschaltkreis und/oder als Schaltkreis mit zusätzlichen Logikfunktionen, beispielsweise als Mikrorechner ausgebildet ist. Der Speicher SP enthält einen ersten Speicherbereich SP1, in dem die dem Teilnehmer zugeordnete Zustandsnummer Z1 gespeichert ist und einen zweiten Speicherbereich SP2, in dem eine dem Teilnehmer zugeordnete Teilnehmernummer T1 gespeichert ist. Während die Teilnehmernummer T1 über eine Steuereinheit zu einem Endgerät von der Chipkarte CK ausgelesen werden kann, ist die Zustandsnummer Z1 von außen unzugänglich gespeichert.

Beim Einschieben der Chipkarte CK in ein Endgerät wird zur Überprüfung der Chipkarte aus dem Speicherbereich SP1 die Zustandsnummer Z1 und gegebenenfalls auch die Teilnehmernummer T1 ausgelesen und einem Vergleicher V in der Steuereinheit ST zugeführt. Von dem Endgerät oder einer mit diesem verbundenen Zentralstelle wird der Chipkarte CK eine Prüfnummer P zugeführt, die zumindest die der Zustandsnummer Z1 entsprechende Zustandsnummer Z2 und die der Teilnehmernummer T1 entsprechende Teilnehmernummer T2 enthält. Die Übertragung der Zustandsnummer Z2 und gegebenenfalls auch der Teilnehmernummer T2 kann durch die Signale Z2' bzw. T2' verschlüsselt erfolgen. Auf der Chipkarte CK ist eine Entschlüsselungseinheit E vorgesehen, die die Zustandsnummer Z2 und die Teilnehmernummer T2 im Klartext zur Verfügung stellt und ebenfalls dem Vergleicher V zuführt. Bei Übereinstimmung der Zustandsnummern Z1 und Z2 und der Teilnehmernummern T1 und T2 gibt der Vergleicher V ein Vergleichssignal VS ab, das dem Endgerät und gegebenenfalls der Zentralstelle zugeführt wird und das anzeigt, daß die Chipkarte CK gültig ist. Falls das Vergleichssignal VS nicht abgegeben wird, wird die Chipkarte CK gesperrt oder abgewiesen.

Die Zustandsnummern Z1 und Z2 umfassen mindestens zwei Binärzeichen und werden bei der Vergabe statistisch ermittelt. Beim Verlust einer Chipkarte CK wird dem Teilnehmer eine neue Chipkarte CK ausgegeben, die im Speicherbereich SP2 dieselbe Teilnehmernummer T1 enthält, jedoch im Speicherbereich SP1 eine andere Zustandsnummer Z1 enthält, so daß diese Chipkarte CK nur dann benutzt werden kann, wenn in der Sperrdatei die Prüfnummer P mit der neuen Zustandsnummer Z1 gespeichert ist.

Bezugszeichenliste

CK Chipkarte

SP Speicher

SP1 erster Speicherbereich

Z1,Z2 Zustandsnummern

SP2 zweiter Speicherbereich

T1, T2 Teilnehmernummern

V Vergleicher

ST Steuereinheit

P Prüfnummer

Z2', T2' Signale

E Entschlüsselungseinheit

VS Vergleichssignal

Ansprüche

1. Verfahren zum Überprüfen von Chipkarten hinsichtlich der Gültigkeit, bei dem auf der Chipkarte eine Teilnehmernummer gespeichert ist und bei dem die Teilnehmernummer und eine weitere Nummer bei der Überprüfung der Gültigkeit der Chipkarte mit einer in einer Sperrdatei gespeicherten Prüfnummer verglichen wird, **dadurch gekennzeichnet**, daß zusätzlich zu der Teilnehmernummer (T1) auf der Chipkarte (CK) eine Zustandsnummer (Z1) unveränderbar gespeichert ist, die nur innerhalb der Chipkarte (CK) übertragen werden kann und daß auf der Chipkarte (CK) die Zustandsnummer (Z1) mit einer eingegebenen und zur Chipkarte (CK) übertragenen Zustandsnummer (Z2) verglichen wird, um die Gültigkeit zu überprüfen.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß auf der Chipkarte (CK) sowohl die Teilnehmernummber (T1) als auch die Zustandsnummer (Z2) mit einer eingegebenen und zur

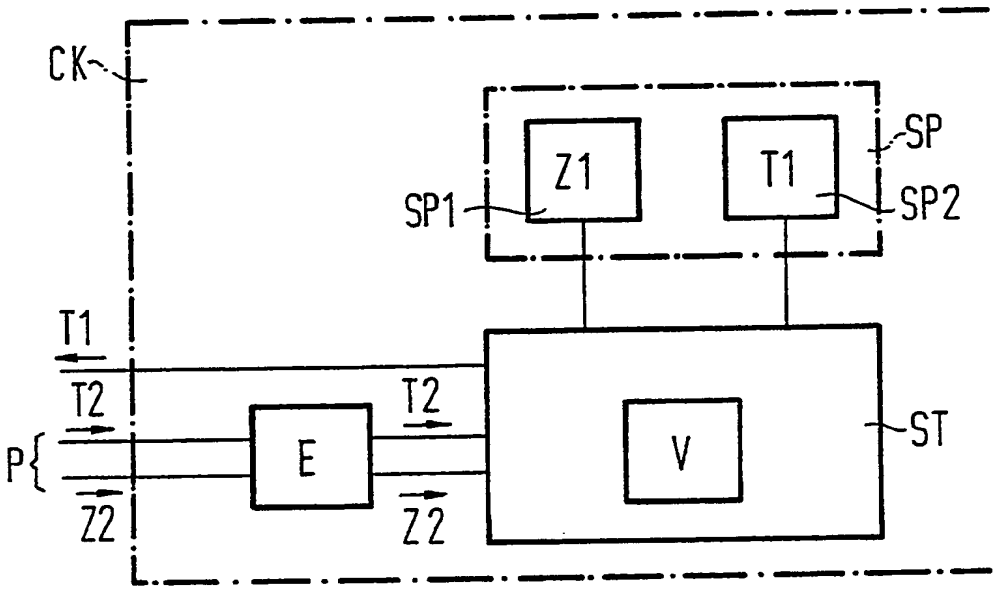
Chipkarte (CK) übertragenen in einer Prüfnummer - (P) enthaltenen Teilnehmernummer (T2) bzw. Zustandsnummer (Z2) verglichen wird.

3. Verfahren nach Anspruch 1 oder Anspruch 2, **dadurch gekennzeichnet**, daß die Zustandsnummer (Z1) mindestens zwei Binärzeichen umfaßt.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet** , daß zumindest die in der Prüfnummer (P) enthaltene Zustandsnummer (Z2) verschlüsselt zur Chipkarte (CK) übertragen wird.

5. Anordnung zur Durchführung des Verfahrens nach Anspruch 1, **dadurch gekennzeichnet**, daß auf der Chipkarte (CK) ein Speicher (SP) mit einem von außen unzugänglichen ersten Speicherbereich (SP1) für die Zustandsnummer (Z1) und einem zweiten Speicherbereich (SP2) für die Teilnehmernummer (T1) und eine Steuereinheit (ST) vorgesehen sind, die einen Vergleicher (V) enthält, der die eingegebene Zustandsnummer (Z2) mit der auf der Chipkarte (CK) gespeicherten Zustandsnummer - (Z1) vergleicht und ein Vergleichssignal (VS) abgibt, wenn beide übereinstimmen.

6. Anordnung nach Anspruch 5, **dadurch gekennzeichnet**, daß die Chipkarte (CK) eine Entschlüsselungseinheit (E) für die eingegebene Zustandsnummer (Z2) enthält.


CK
SP
Z1
T1
SP1
SP2
T1
T2
T2
P
E
V
ST
Z2
Z2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 203 543**
A3

(12) # EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **86106997.9**

(51) Int. Cl.4: **G07F 7/10**

(22) Anmeldetag: **23.05.86**

(30) Priorität: **31.05.85 DE 3519554**

(43) Veröffentlichungstag der Anmeldung:
03.12.86 Patentblatt 86/49

(84) Benannte Vertragsstaaten:
DE FR GB IT SE

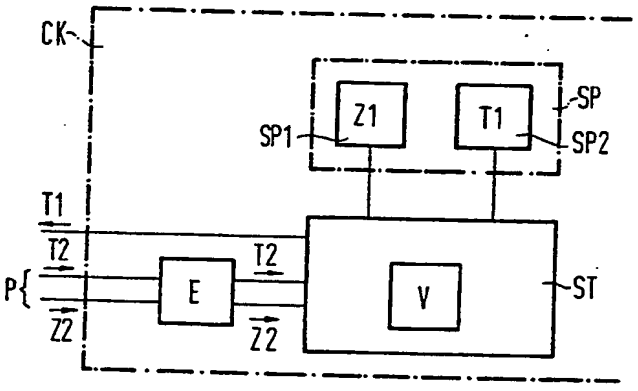
(88) Veröffentlichungstag des später veröffentlichten Recherchenberichts: **20.04.88 Patentblatt 88/16**

(71) Anmelder: **Siemens Aktiengesellschaft Berlin und München**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Krivachy, Thomas, Dr.-Phil.**
Buchauerstrasse 39
D-8000 München 71(DE)

(54) **Verfahren und Anordnung zum Überprüfen von Chipkarten.**

(57) Die Überprüfung von Chipkarten (CK) hinsichtlich der Berechtigung des Zugangs zu einem Chipkartensystem erfolgt dadurch, daß einem Teilnehmer neben einer festen Teilnehmernummer (T1) oder Kontonummer eine ihm unbekannte Zustandsnummer (Z1) zugeteilt wird. Die Zustandsnummer (Z1) ist auf der Chipkarte (CK) derart gespeichert, daß sie nicht von außen ausgelesen werden kann. Zur Überprüfung der Berechtigung wird der Chipkarte (CK) von der Zentralstelle oder einem Endgerät die Zustandsnummer (Z2) zugeführtund auf der Chipkarte (CK) mit der dort gespeicherten Zustandsnummer (Z1) verglichen. Zusätzlich zu der Zustandsnummer (Z1) kann auch die Teilnehmernummer (T1) verglichen werden. Die Zustandsnummer (Z2) und gegebenenfalls die Teilnehmernummer (T2) können verschlüsuselt zur Chipkarte (CK) übertragen werden.



EP 0 203 543 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 86106997.9

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.4)
Y	EP - A2 - 0 138 386 (KABUSHIKI KAISHA TOSHIBA) * Gesamt * --	1,5,6	G 07 F 7/10
Y	US - A - 4 105 156 (DETHLOFF) * Gesamt * --	1,5,6	
A	IEEE SPECTRUM, February 1984, New York STEPHEN B. WEINSTEIN, "Smart Credit Cards: The Answer to Cashless Shopping" Seiten 43-49 * Gesamt * ----	1,5	

RECHERCHIERTE SACHGEBIETE (Int. Cl.4)

G 06 K 19/00
G 07 F 7/00

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt.

Recherchenort	Abschlußdatum der Recherche	Prüfer
WIEN	09-02-1988	BEHMER

KATEGORIE DER GENANNTEN DOKUMENTEN

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur
T : der Erfindung zugrunde liegende Theorien oder Grundsätze

E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPA Form 1503 03 82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 203 543 B1**

(12) # EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag der Patentschrift: **13.11.91**

(51) Int. Cl.5: **G07F 7/10**

(21) Anmeldenummer: **86106997.9**

(22) Anmeldetag: **23.05.86**

(54) **Verfahren und Anordnung zum Überprüfen von Chipkarten.**

(30) Priorität: **31.05.85 DE 3519554**

(43) Veröffentlichungstag der Anmeldung:
03.12.86 Patentblatt 86/49

(45) Bekanntmachung des Hinweises auf die Patenterteilung:
13.11.91 Patentblatt 91/46

(84) Benannte Vertragsstaaten:
DE FR GB IT SE

(56) Entgegenhaltungen:
EP-A- 0 138 386
US-A- 4 105 156

IEEE SPECTRUM, February 1984, New York STEPHEN B. WEINSTEIN, "Smart Credit Cards: The Answer to Cashless Shopping",Seiten 43-49

(73) Patentinhaber: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
W-8000 München 2(DE)

(72) Erfinder: **Krivachy, Thomas, Dr.-Phil.**
Buchauerstrasse 39
W-8000 München 71(DE)

EP 0 203 543 B1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zum Überprüfen von Chipkarten entsprechend dem Oberbegriff des Patentanspruches 1. Weiterhin bezieht sich die Erfindung auf eine Anordnung zur Durchführung des Verfahrens.

Es ist bereits allgemein bekannt, Chipkarten als elektronisches Zahlungsmittel zu verwenden. Die Chipkarten werden beispielsweise an sogenannten POS (Point of Sales)-Endgeräten oder an öffentlichen Kartentelefonen benutzt. Die Chipkarten enthalten mindestens einen integrierten Schaltkreis, der als Speicherschaltkreis und/oder als Schaltkreis mit zusätzlichen Logikfunktionen, beispielsweise als Mikrorechner ausgebildet sein kann.

Wenn Chipkarten als elektronisches Zahlungsmittel oder auch als Berechtigungskarten für den Zugriff zu bestimmten Daten verwendet werden, werden die Chipkarten durch Vergleich mit Daten abhandengekommener Chipkarten, welche in Sperrdateien hinterlegt sind, aus Sicherheitsgründen auf ihre Echtheit und Gültigkeit überprüft. Bei Verlust der Chipkarte meldet der Kunde seine Konto- oder Teilnehmernummer an den Systembetreiber, der diese Nummer dann sperrt (Hot List) und dem Kunden eine neue Nummer zuteilt (siehe IEEE Spectrum, February 1984, New York - Stephen B. Weinstein, "Smart credit cards: the answer to cashless shopping", Seiten 43 bis 49). Bei bestimmten Nummern, z.B. der Fernmeldekontonummer, Personalnummer einer Firma oder Versicherungsnummer ist eine Änderung der Nummer oft mit erheblichem Aufwand verbunden oder unmöglich.

Chipkarten mit einer festen von einer Bank vorgegebenen persönlichen Identifikationsnummer (PIN) oder einer vom Kunden individuell wählbaren Nummer (PIN) sind üblich. Die vom Kunden individuell wählbare Nummer kann dabei mehrmals geändert werden, ohne daß die Teilnehmernummer geändert werden muß. Nach Ablauf der Karte wird hierbei dem berechtigten Benutzer beispielsweise von der Bank ein neuer Sicherheitscode ausgehändigt. Die Neuinitialisierung der Karte mit neuer vom Kunden wählbarer PIN ist damit möglich. Nach erfolgter Neuinitialisierung ist der Sicherheitscode wertlos. Karten zugriffe erfolgen wie gewohnt über die neugewählte PIN(US-A-4105 156).

Der Erfindung liegt die Aufgabe zugrunde, ein verfahren zum Überprüfen der Gültigkeit von Chipkarten anzugeben, bei dem die Sicherheit weiter erhöht wird, ohne daß bei dem Verlust einer Chipkarte die Teilnehmernummer geändert werden muß.

Erfindungsgemäß wird die Aufgabe bei dem verfahren der eingangs genannten Art durch die im kennzeichnenden Teil des Patentanspruchs 1 angegebenen Merkmale gelöst.

Sowohl dem Chipkartensystem als auch der Chipkarte sind sowohl die Teilnehmernummer als auch die Zustandsnummer bekannt, wogegen der Kunde nur die Teilnehmernummer kennt. Die heutige Technologie ermöglicht es, auf den Chipkarten Speicherbereiche festzulegen, deren Daten niemals gelöscht, geändert oder ausgelesen werden können, die aber auf der Chipkarte einen Vergleich zwischen einer eingegebenen und der abgespeicherten Nummer durchführen. Im Sinne der Erfindung bedeutet das, daß die Zustandsnummer von niemandem ausgelesen und damit kein Mißbrauch betrieben werden kann. Falls der Kunde veranlaßt, daß die ihm ausgegebene Chipkarte gesperrt werden soll, weil er sie verloren hat oder weil der Verdacht auf Vorhandensein einer weiteren, aber gefälschten Karte besteht, dann kann er gemäß der Erfindung eine neue Chipkarte mit der ursprünglichen Teilnehmernummer aber mit einer anderen Zustandsnummer erhalten.

Bei einer bevorzugten Ausführungsform der Erfindung wird auf der Chipkarte nicht nur die Zustandsnummer, sondern auch die Teilnehmernummer mit einer zur Chipkarte übertragenen Prüfnummer verglichen.

Die Zustandsnummer enthält mindestens ein Bit. Aus Sicherheitsgründen ist es jedoch empfehlenswert, daß die Zustandsnummer mindestens zwei Binärzeichen umfaßt. Aus Sicherheitsgründen können die Zustandsnummern statistisch vergeben werden, d. h. bei Verlust einer Chipkarte wird bei der neuen Chipkarte die Zustandsnummer nicht um 1 erhöht oder erniedrigt, sondern statistisch ausgewählt.

Zur Erhöhung der Sicherheit wird in einer weiteren Variante der Erfindung die zur Chipkarte übertragene Prüfnummer, bestehend aus der Tei lnehmernummer und der variablen Zustandsnummer oder nur die Zustandsnummer nicht im Klartext, sondern verschlüsselt übertragen. Auf der Chipkarte wird die Prüfnummer dann entschlüsselt und die Zustandsnummer und gegebenenfalls auch die Teilnehmernummer wird mit der dort gespeicherten Zustandsnummer bzw. Teilnehmernummer verglichen. In der Sperrdatei ist der Schlüssel für jeden Teilnehmer bekannt und der verschlüsselte Text kann in Klartext umgewandelt werden.

Eine bevorzugte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß auf der Chipkarte ein Speicher mit einem von außen unzugänglichen ersten Speicherbereich für die Zustandsnummer und einem zweiten Speicherbereich für die Teilnehmernummer und eine Steuereinheit vorgesehen sind, die eine eingegebene Prüfnummer mit der Zustandsnummer vergleicht und ein Vergleichssignal abgibt.

Zur Entschlüsselung der zur Chipkarte übertra-

genen Prüfnummer, zumindest der Zustandsnummer ist bei einer weiteren bevorzugten Ausführungsform eine Entschlüsselungseinrichtung auf der Chipkarte vorgesehen.

Eine Durchführung des Verfahrens gemäß der Erfindung wird im folgenden anhand einer Anordnung näher beschrieben.

Die Figur zeigt ein Blockschaltbild einer Chipkarte.

Die Chipkarte CK ist in bekannter Weise mit einem elektronischen Schaltkreis versehen, der als Speicherschaltkreis und/oder als Schaltkreis mit zusätzlichen Logik-funktionen, beispielsweise als Mikrorechner ausgebildet ist. Der Speicher SP enthält einen ersten Speicherbereich SP1, in dem die dem Teilnehmer zugeordnete Zustandsnummer Z1 gespeichert ist und einen zweiten Speicherbereich SP2, in dem eine dem Teilnehmer zugeordnete Teilnehmernummer T1 gespeichert ist. Während die Teilnehmernummer T1 über eine Steuereinheit zu einem Endgerät von der Chipkarte CK ausgelesen werden kann, ist die Zustandsnummer Z1 von außen unzugänglich gespeichert.

Beim Einschieben der Chipkarte CK in ein Endgerät wird zur Überprüfung der Chipkarte aus dem Speicherbereich SP1 die Zustandsnummer Z1 und gegebenenfalls auch die Teilnehmernummer T1 ausgelesen und einem Vergleicher V in der Steuereinheit ST zugeführt. Von dem Endgerät oder einer mit diesem verbundenen Zentralstelle wird der Chipkarte CK eine Prüfnummer P zugeführt, die zumindest die der Zustandsnummer Z1 entsprechende Zustandsnummer Z2 und die der Teilnehmernummer T1 entsprechende Teilnehmernummer T2 enthält. Die Übertragung der Zustandsnummer Z2 und gegebenenfalls auch der Teilnehmernummer T2 kann durch die Signale Z2' bzw. T2' verschlüsselt erfolgen. Auf der Chipkarte CK ist eine Entschlüsselungseinheit E vorgesehen, die die Zustandsnummer Z2 und die Teilnehmernummer T2 im Klartext zur Verfügung stellt und ebenfalls dem Vergleicher V zuführt. Bei Übereinstimmung der Zustandsnummern Z1 und Z2 und der Teilnehmernummern T1 und T2 gibt der Vergleicher V ein Vergleichssignal ab, das dem Endgerät und gegebenenfalls der Zentralstelle zugeführt wird und das anzeigt, daß die Chipkarte CK gültig ist. Falls das Vergleichssignal nicht abgegeben wird, wird die Chipkarte CK gesperrt oder abgewiesen.

Die Zustandsnummern Z1 und Z2 umfassen mindestens zwei Binärzeichen und werden bei der Vergabe statistisch ermittelt. Beim Verlust einer Chipkarte CK wird dem Teilnehmer eine neue Chipkarte CK ausgegeben, die im Speicherbereich SP2 dieselbe Teilnehmernummer T1 enthält, jedoch im Speicherbereich SP1 eine andere Zustandsnummer Z1 enthält, so daß diese Chipkarte CK nur dann benutzt werden kann, wenn in der Sperrdatei des Chipkartensystems die Prufnummer P mit der neuen Zustandsnummer Z1 gespeichert ist.

Patentansprüche

1. Verfahren zum Überprüfen von Chipkarten (CK) hinsichtlich der Gültigkeit, bei dem auf der Chipkarte (CK) eine dem Teilnehmer bekannte Teilnehmernummer (T1) gespeichert ist und bei dem die Teilnehmernummer (T1) und eine weitere Nummer (Z1) auf der Chipkarte (CK) bei der Überprüfung der Gültigkeit der Chipkarte (CK) mit einer in einer Sperrdatei des Chipkartensystems gespeicherten Prüfnummer (P) verglichen wird, **dadurch gekennzeichnet,** daß zusätzlich zu der Teilnehmernummer (T1) auf der Chipkarte (CK), eine dem Benutzer unbekannte Zustandsnummer (Z1) unveränderbar gespeichert ist, die nur innerhalb der Chipkarte (CK) übertragen werden kann und daß auf der Chipkarte (CK) die Zustandsnummer (Z1) mit einer eingegebenen und zur Chipkarte (CK) übertragenen Zustandsnummer (Z2) verglichen wird, um die Gültigkeit zu überprüfen.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß auf der Chipkarte (CK) sowohl die Teilnehmernummer (T1) als auch die Zustandsnummer (Z2) mit einer eingegebenen und zur Chipkarte (CK) übertragenen in einer Prüfnummer (P) enthaltenen leilnehmernummer (T2) bzw. Zustandsnummer (Z2) verglichen wird.

3. Verfahren nach Anspruch 1 oder Anspruch 2, **dadurch gekennzeichnet,** daß die Zustandsnummer (Z1) mindestens zwei Binärzeichen umfaßt.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** daß zumindest die in der Prüfnummer (P) enthaltene Zustandsnummer (Z2') verschlüsselt zur Chipkarte (CK) übertragen wird.

5. Anordnung zur Durchführung des Verfahrens nach Anspruch 1, **dadurch gekennzeichnet,** daß auf der Chipkarte (CK) ein Speicher (SP) mit einem von außen unzugänglichen ersten Speicherbereich (SP1) für die Zustandsnummer (Z1) und einem zweiten Speicherbereich (SP2) für die leilnehmernummer (T1) und eine Steuereinheit (ST) vorgesehen sind, die einen Vergleicher (V) enthält, der die zugeführte Zustandsnummer (Z2) mit der auf der Chipkarte

(CK) gespeicherten Zustandsnummer (Z1) vergleicht und ein Vergleichssignal abgibt, wenn beide übereinstimmen.

6. Anordnung nach Anspruch 5, **dadurch gekennzeichnet,** daß die Chipkarte (CK) eine Entschlüsselungseinheit (E) für die zugeführte Prüfnummer (P), bestehend aus Teilnehmernummer (T2') und Zustandsnummer (Z2'), oder für die zugeführte Zustandsnummer (Z2') enthält.

Claims

1. Method for testing chip cards (CK) with respect to validity in which a subscriber number (T1) known to the subscriber is stored on the chip card (CK) and in which the subscriber number (T1) and a further number (Z1) on the chip card (CK) is compared when testing the validity of the chip card (CK) with a test number (P) stored in a locked file of the chip card system, characterised in that, in addition to the subscriber number (T1), a status number (Z1) not known to the user is stored in an unchangeable manner on the chip card (CK), which status number can only be transmitted within the chip card (CK), and in that on the chip card (CK) the status number (Z1) is compared with an input status number (Z2) transmitted to the chip card (CK), in order to test the validity.

2. Method according to Claim 1, characterised in that on the chip card (CK) both the subscriber number (T1) and the status number (Z2) are compared with an input subscriber number (T2) or status number (T2) which is transmitted to the chip card (CK) and contained in a test number (P).

3. Method according to Claim 1 or 2, characterised in that the status number (Z1) comprises at least two binary characters.

4. Method according to one of Claims 1 to 3, characterised in that at least the status number (Z2') contained in the test number (P) is transmitted to the chip card (CK) in encrypted form.

5. Arrangement for carrying out the method according to Claim 1, characterised in that on the chip card (CK) a memory (SP) having a first memory area (SP1), inaccessible from the outside, for the status number (Z1) and a second memory area (SP2) for the subscriber number (T1) and a control unit (ST) are provided, said control unit (ST) containing a comparator (V) which compares the supplied status number (Z2) with the status number (Z1) stored on the chip card (CK) and emits a comparison signal if both coincide.

6. Arrangement according to Claim 5, characterised in that the chip card (CK) contains a decryption unit (E) for the supplied test number (P), consisting of subscriber number (T2') and status number (Z2'), or for the supplied status number (Z2').

Revendications

1. Procédé pour contrôler la validité de cartes à puce (CK), selon lequel un numéro d'abonné (T1) connu de l'abonné est mémorisé sur la carte à puce (CK) et selon lequel le numéro d'abonné (T1) et un autre numéro (Z1) situés sur la carte à puce (CK) sont comparés, lors du contrôle de la validité de cette carte à puce, à un numéro de contrôle (P) mémorisé dans un fichier de blocage du système de cartes à puce, caractérisé par le fait qu'en plus du numéro d'abonné (T1), un numéro d'état (Z1) inconnu de l'utilisateur et qui peut être transmis à l'intérieur de la carte à puce (CK) est mémorisé, d'une manière non modifiable, sur la carte à puce (CK) et que, dans la carte à puce (CK), le numéro d'état (Z1) est comparé à un numéro d'état introduit (Z2), transmis à la carte à puce (CK), pour le contrôle de la validité.

2. Procédé suivant la revendication 1, caractérisé par le fait que sur la carte à puce (CK), aussi bien le numéro d'abonné (T1) que le numéro d'état (Z2) sont comparés à un numéro d'abonné (T2) et à un numéro d'état (Z2) introduits, transmis à la carte à puce (CK) et contenus dans un numéro de contrôle (P).

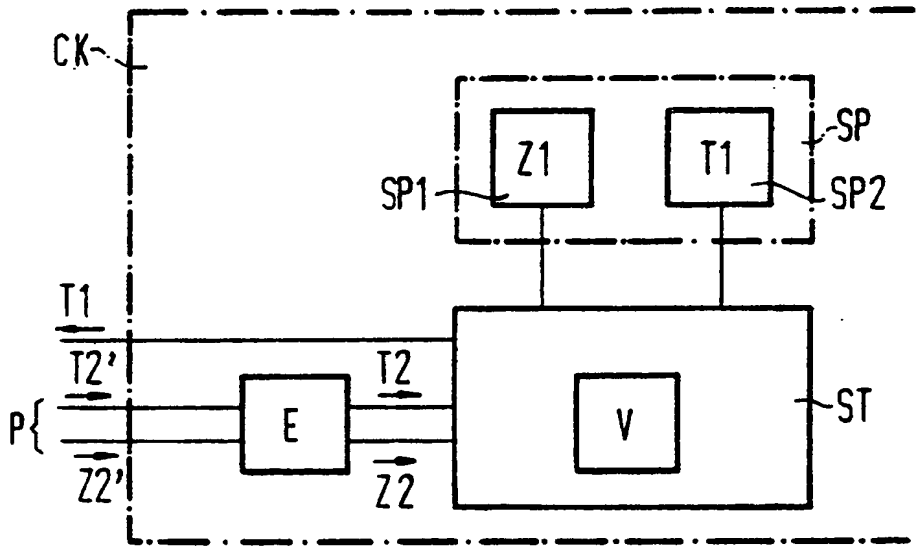
3. Procédé suivant la revendication 1 ou 2, caractérisé par le fait que le numéro d'état (Z1) comprend au moins deux signes binaires.

4. Procédé suivant l'une des revendications 1 à 3, caractérisé par le fait qu'au moins le numéro d'état (Z2') contenu dans le numéro de contrôle (P) est transmis sous forme codé à la carte à puce (CK).

5. Dispositif pour la mise en oeuvre du procédé suivant la revendication 1, caractérisé par le fait que dans la carte à puce (CK) il est prévu une mémoire (SP) comportant une première zone de mémoire (SP1), accessible de l'extérieur, pour le numéro d'état (Z1) et une secon-

de zone de mémoire (SP2) pour le numéro d'abonné (T1), et une unité de commande (ST), qui contient un comparateur (V) qui compare le numéro d'état (Z2) envoyé, au numéro d'état (Z1) mémorisé dans la carte à puce (CK), et délivre un signal de comparaison lorsque ces deux numéros d'état sont identiques.

6. Dispositif suivant la revendication 5, caractérisé par le fait que la carte à puce (CK) comporte une unité de décodage (E) pour le numéro de contrôle (P) envoyé, qui est constitué par un numéro d' abonné (T2') et un numéro d'état (Z2'), ou pour le numéro d'état envoyé (Z2').


CK
SP
Z1
T1
SP1
SP2
T1
T2'
T2
P
E
V
ST
Z2'
Z2